

# Illumina Proactive Technical Note

The benefits of Illumina Proactive, and instructions on how to implement performance monitoring with Illumina sequencing instruments.

## Table of contents

Maximizing operational efficiency through Illumina Proactive	2
Benefits of Illumina Proactive	2
Maximize instrument uptime	2
Troubleshoot runs more efficiently	2
What is instrument performance data and why is it important?	2
How to enable Illumina Proactive	3
Requirements for enabling Illumina Proactive	3
Instructions for enabling Illumina Proactive	3
Data security considerations	3
No inbound ports	3
Software restriction policy	3
Enhanced machine experience toolkit	3
Windows security updates	3
Security in transit	3
Encryption at rest	3
Data center security	4
Frequently asked questions about data security	4
Appendix	4
Universal settings	4
Antivirus configuration	6
Operating systems configurations	6
Windows updates	7
Third-party software	7
User behavior	7
Group policy application	7
Password management	7
Administrative rights and privileges	7
Instrument-specific settings	7
Instrument performance data types	9
References	12

## Maximizing operational efficiency through Illumina Proactive

Illumina provides a wide range of next-generation sequencing (NGS) instruments that have become the core production technology for many laboratories. Whether a user is operating a large sequencing center or a small research lab with a single instrument, reliable instrument operation and management are critical for optimal usage with maximum throughput.

To achieve this goal, Illumina provides Illumina Proactive, a monitoring service in which instrument performance data from each run are sent to Illumina to enable proactive maintenance. All Illumina sequencing instruments are designed to capture performance data, while the type of metrics used to monitor performance depends on the software version. By enabling Illumina Proactive, users facilitate troubleshooting with more accurate diagnosis of failures and detection of failure risks. Furthermore, Illumina Proactive can increase instrument uptime, improve operational efficiency, and reduce the risk of lost resources.

This technical note explains the benefits of instrument performance monitoring, instructs on how to enable Illumina Proactive, and answers frequently asked questions about data security.

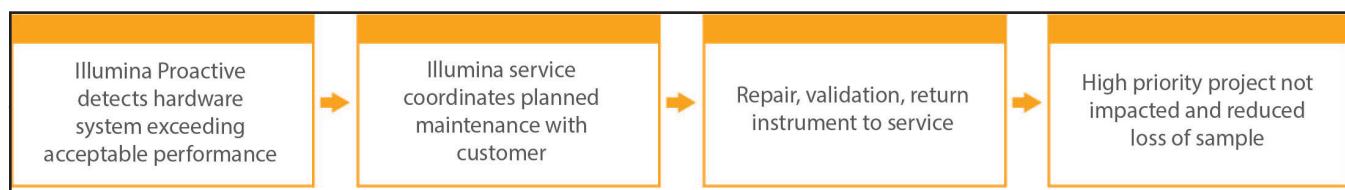
## Benefits of Illumina Proactive

### Maximize instrument uptime

Preemptive detection and notification of elevated instrument failure risk can reduce unplanned downtime and allow users to schedule required component replacements at their convenience. This capability has been enabled for several Illumina instrument components and will continue to be expanded to others.

### Troubleshoot runs more efficiently

Requiring users to locate, download, and send required information can cause unnecessary delays. On the other hand, direct access to instrument performance parameters allows the Illumina Service and Support team to diagnose and troubleshoot instrument issues quickly. In addition, historical performance monitoring supports efficient troubleshooting, and sometimes, preemptive instrument repair.



**Figure 1: Sample of how Illumina Proactive can benefit laboratories through detection of risk failure and facilitated troubleshooting**—Routine monitoring of system performance data results in detection of failure risk for optical hardware, resulting in planned maintenance around a high priority project. A potentially expensive loss of time, effort, and sample is avoided.

## What is instrument performance data and why is it important?

Instrument performance data refers to any metric that can characterize the operational performance of the sequencing instrument, including software logs, instrument configurations, and other file types. Sequencing data are not included in this category, and are not accessible or reported through the same data stream. Instrument performance data can support failure risk prediction, failure detection, and performance issue troubleshooting in various ways (Table 1).

**Table 1: Different types of instrument performance data**

	Run performance data	Instrument configuration data	Run configuration data
Data collected	Q-scores, error rates, instrument operational logs	Instrument serial number, software version	Run parameters, reagent and flow cell lot numbers, primary analysis set-up and configuration.
Value to Illumina Service team	Failure risk prediction, failure detection	Run troubleshooting	Run troubleshooting
Value to user	Enables analysis of error and warning notifications regarding optical, mechanical, thermal, and fluidic system performance	Enables assessment of whether software version, instrument type, or other hardware variables may be contributing to performance issues	Informs on roles of lot numbers, experiment type, and other experimental variables that contribute to performance issues

## How to enable Illumina Proactive

For each system, instrument performance monitoring is configured in the control software by the user. User manuals provide details on how to enable or disable the delivery of instrument performance data. For greater detail on universal and instrument-specific network configurations, refer to the Universal Settings and Instrument-Specific Settings sections in this document.

### Requirements for enabling Illumina Proactive:

- Port 443, 80, and 8080
- BaseSpace Domains for each region
- Connection to a 1 GB network switch to accommodate delivery. Additional details regarding networking and bandwidth are provided in site prep guides for specific instruments.
- Software must be configured to enable performance monitoring

### Instructions for enabling Illumina Proactive:

1. Make sure that any concerns regarding information security are addressed by appropriate IT representatives, and that all institutional requirements are met.
2. Confirm current system instrument performance monitoring settings. Some instruments may already be enabled by default. See instrument performance monitoring settings (Table 5).
3. Enable “Send Instrument Performance Data to Illumina” checkbox prior to starting a run. All Illumina instruments should provide this option in the user interface, although the exact wording may vary.

## Data security considerations

Data security is a top priority for Illumina customers. As a result of consistent effort, security profiles for Illumina operating systems improve over time as new systems are designed and new threats to information are identified.

### No inbound ports

Illumina sequencing systems do not require inbound ports from the Internet. Illumina recommends blocking these ports, which reduces the possibility of reaching the login screen via the internet. This security measure reduces access to the operating system from remote locations.

### Software restriction policy

NovaSeq™ and iSeq™ Systems have a feature called software restriction policy (SRP), which limits the applications run on Illumina computers to those that Illumina has approved (allow-listed). This restriction prevents any malware from being executed, even if it infiltrates the system, because SRP protection will not allow execution, regardless of how files appear to the user (ie, malware may appear as an image file, or excel spreadsheet).

### Enhanced machine experience toolkit

NovaSeq Systems include a feature called enhanced machine experience toolkit (EMET). Designed by Microsoft, EMET provides an additional layer of security for Microsoft Windows. With an interface that can be used to adjust Windows security features, EMET is an additional, complementary defense tool placed between the firewall and user-selected antivirus software.

### Windows security updates

Illumina recommends that all Windows security updates be applied regularly. However, this feature is not enabled by default. Instructions for enabling security updates are provided in the Microsoft Security Update Guide.<sup>1</sup>

### Security in transit

Instruments communicate with BaseSpace™ Sequence Hub through a web-based application program interface (API). All traffic between the sequencing instrument and BaseSpace Sequence Hub uses Transport Layer Security (TLS), an internet standard that encrypts sensitive communications as they pass over the internet. All service methods require API key signatures, and service is refused to all others.

### Encryption at rest

Data that are stored in persistent storage systems are referred to as being “at rest.” BaseSpace Sequence Hub uses Advanced Encryption System (AES)-256 to protect data at rest. AES-256 is a specification for the encryption of electronic data, established by the US National Institutes of Standards and Technology (NIST).<sup>2</sup>

## Data center security

BaseSpace Sequence Hub is built on preexisting cloud infrastructure provided by Amazon Web Services (AWS), and inherits controls that have allowed BaseSpace Sequence Hub to achieve ISO 27001<sup>3</sup> and Health Insurance Portability and Accountability Act (HIPAA) compliance. Illumina software as a service (SaaS) products are designed and operated in keeping with best practices and laws around data protection and data handling, including General Data Protection Regulation (GDPR).<sup>4</sup> Customers should determine GDPR responsibilities for use of their own personal data. More details on cloud security, privacy, HIPAA, and GDPR are provided in separate papers.<sup>5,6</sup>

## Frequently asked questions about data security

**Will my sequence data also be sent to Illumina if I enable Illumina Proactive?**

No. Only instrument performance data, which includes software logs and instrument configurations as described above, are sent by the instrument to Illumina. Sequencing run data are not sent and are not accessible through this service. Various features distinguish the connectivity between instrument performance monitoring and sequence data analysis (Table 2).

**Table 2: BaseSpace Sequence Hub connectivity options**

Attribute	Illumina Proactive mode	Run monitoring mode	BaseSpace Sequence Hub Analysis mode
Connection type	One-time instrument configuration	Per-run user connection	Per-run user connection
Requires internet connection	X	X	X
Includes instrument configuration and operational logs <sup>a</sup>	X	X	X
Requires BaseSpace Sequence Hub login		X	X
Includes sequence data [BCL] files			X

a. For details around specific instrument configuration and operational logs, please refer to the Instrument-specific settings section in the appendix.

**Will sending my instrument performance data to Illumina enable all types of failure risk to be proactively detected?**

No. Instrument performance monitoring has successfully enabled proactive maintenance on a number of cases to date. As more data become available, the capabilities of this service will continue to be expanded and improved across the Illumina portfolio of sequencing products.

**Will I need to log in to my BaseSpace Sequence Hub to enable this service?**

No. For instrument performance data mode, only a network connection to Illumina is needed. Because instrument performance data and sequencing data are sent independently of each other, a BaseSpace Sequence Hub login is not required.

**My Information Security team requires additional technical information prior to enabling this service. Are there additional resources available?**

Yes. Additional details and an overview of data security considerations are provided in this document. Links to Site Prep Guides for each system are also available in the appendix. More information on SaaS security is provided in the BaseSpace Sequence Hub security paper.<sup>5</sup>

**Is Illumina Proactive compliant with GDPR?**

Yes. Illumina SaaS products are designed and operated to comply with global laws, including GDPR.

**Are there other best practices that Illumina recommends concerning data security?**

Illumina strongly recommends that sample-specific information be omitted from the name of the experiment or sample ID.

## Appendix

The remaining sections contain information on requirements that your IT department needs to know to implement Illumina Proactive.

### Universal settings

Several integration settings are common to all Illumina systems for implementing Illumina Proactive or integrating with BaseSpace Sequence Hub.

**Table 3: Instrument connectivity endpoints**

Instance	Address
US Enterprise	{domain}.basespace.illumina.com
	api.basespace.illumina.com
	basespace-data-east.s3-external-1.amazonaws.com
	basespace-data-east.s3.amazonaws.com
	instruments.sh.basespace.illumina.com
	login.illumina.com
EU Enterprise	use1.platform.illumina.com <sup>a</sup>
	{domain}.euc1.sh.basespace.illumina.com
	api.euc1.sh.basespace.illumina.com
	euc1-prd-seq-hub-data-bucket.s3.eu-central-1.amazonaws.com
	euc1-prd-seq-hub-data-bucket.s3-eu-central-1.amazonaws.com
	instruments.sh.basespace.illumina.com
AUS Enterprise	login.illumina.com
	euc1.platform.illumina.com <sup>a</sup>
	{domain}.aps2.sh.basespace.illumina.com
	api.aps2.sh.basespace.illumina.com
	instruments.sh.basespace.illumina.com
	aps2-sh-prd-seq-hub-data-bucket.s3.ap-southeast-2.amazonaws.com
Canada Enterprise	login.illumina.com
	aps2.platform.illumina.com <sup>a</sup>
	{domain}.cac1.sh.basespace.illumina.com
	api.cac1.sh.basespace.illumina.com
	instruments.sh.basespace.illumina.com
	cac1-sh-prd-seq-hub-data-bucket.s3.ca-central-1.amazonaws.com
US Basic and Professional	login.illumina.com
	cac1.platform.illumina.com
	basespace.illumina.com
	api.basespace.illumina.com
	basespace-data-east.s3-external-1.amazonaws.com
	basespace-data-east.s3.amazonaws.com
EU Basic and Professional	instruments.sh.basespace.illumina.com
	login.illumina.com
	use1.platform.illumina.com <sup>a</sup>
	euc1.sh.basespace.illumina.com
	api.euc1.sh.basespace.illumina.com
	euc1-prd-seq-hub-data-bucket.s3.eu-central-1.amazonaws.com
AUS Basic and Professional	euc1-prd-seq-hub-data-bucket.s3-eu-central-1.amazonaws.com
	instruments.sh.basespace.illumina.com
	login.illumina.com
	euc1.platform.illumina.com <sup>a</sup>
	aps2.sh.basespace.illumina.com
	api.aps2.sh.basespace.illumina.com

a. URL is only needed for the NextSeq1000 and NextSeq 2000 Sequencing Systems.

**Table 3: Instrument connectivity endpoints, cont.**

Instance	Address	
China Basic and Professional	cnn1.sh.basespace.illumina.com.cn	
	api.cnn1.sh.basespace.illumina.com.cn	
	instruments.sh.basespace.illumina.com.cn	
	cn-sh-cnn1-prod-seq-hub-data-bucket.s3.cn-north-1.amazonaws.com.cn	
	pa.login.illumina.com.cn	
	cnn1.platform.illumina.com.cn	
	cac1.sh.basespace.illumina.com	
Canada Basic and Professional	api.cac1.sh.basespace.illumina.com	
	instruments.sh.basespace.illumina.com	
	cac1-sh-prd-seq-hub-data-bucket.s3.ca-central-1.amazonaws.com	
	login.illumina.com	
	cac1.platform.illumina.com	
Port (outbound)	Port requirements	Purpose
443		BaseSpace Sequence Hub configuration
80		BaseSpace Sequence Hub data upload
8080		Software updates

a. For details around specific instrument configuration and operational logs, please refer to the Instrument specific settings section in the appendix.

Inbound ports are not required or recommended, except for Local Run Manager (LRM). Remote Desktop Protocol (RDP) may be enabled on some systems, by default, and the recommendation is to close all inbound ports, including RDP, unless LRM is noted as a requirement for local allow-listing. LRM does not require internet access, only access to local storage and management resources. The Illumina Security Best Practices Guide provides more information on firewalls and RDP.<sup>7</sup>

## Antivirus configuration

User-selected antivirus software is highly recommended to protect the instrument control computer against viruses. To avoid data loss or interruptions, configure the antivirus software as follows:

- Set for manual scans. Do not allow automatic scans.
- Perform manual scans only when the instrument is not in use.
- Set updates to download without user authorization, but not install.
- Do not update during instrument operation. Update only when the instrument is not running and when it is safe to reboot the instrument control computer.
- Do not reboot the computer automatically upon update.
- Exclude the application directory and data drives from any real-time file system protection. Apply this setting to the C:\Illumina and Z:\ilmn directories.
- Disable Windows Defender. This Windows product can affect the operating system resources used by Illumina software.

## Operating system configurations

Illumina instruments are tested and verified to operate within specifications before shipping. After installation, changes to settings can create performance or security risks. The following configuration recommendations mitigate performance and security risks for the operating system:

- Configure a password that is at least 10 characters, and use local ID policies for additional guidance. Keep a record of the password.
- Illumina does not keep customer login credentials, and unknown passwords cannot be reset.
- An unknown password requires that an Illumina representative restore the factory default, which removes all data from the system and extends the necessary support time.
- Configure Automatic Updates in Windows to prevent updates.
- When connecting to a domain with Group Policy Objects (GPOs), some settings might affect the operating system or instrument software. If the instrument software operates incorrectly, consult your facility IT administrator about possible GPO interference.
- Use the Windows firewall or a network firewall (hardware or software) and disable the Remote Desktop Protocol (RDP). For more information on firewalls and RDP, see the Illumina Security Best Practices Guide.<sup>5</sup>
- Maintain administrative privileges for users. Illumina instrument software is configured to allow user permissions when the instrument is shipped.
- The system has fixed internal IP addresses, which can cause system failure when conflicts occur.
- The control computer is designed to operate Illumina sequencing systems. Web browsing, checking email, reviewing documents, and other nonsequencing activity creates quality and security problems.

## Windows updates

Illumina recommends the application of Critical Security Updates only. To control configuration and operation of the instrument control computer and deliver a more robust operating environment, the default Windows OS has Windows Update turned off. Feature or General Updates on the system can put the system operating environment at risk and is not supported. The Illumina Security Best Practices Guide provides more information on Windows Update alternatives.<sup>5</sup>

## Third-party software

Illumina does not support software beyond what is provided at installation. Do not install Chrome, Java, Box, or any other third-party software that was not provided with the system. Third-party software is untested and can interfere with performance and security. For example, RoboCopy or other synchronization and streaming programs can cause corrupt or missing sequencing data because it interferes with streaming performed by the control software suite.

## User behavior

The instrument control computer is designed to operate Illumina sequencing systems. It should not be used as a general-purpose computer. For quality and security reasons, using the control computer for web browsing, checking email, reviewing documents, or other unnecessary activity is discouraged, as it can result in degraded performance or loss of data.

## Group policy application

When connecting to a domain with Group Policy Objects (GPOs), some settings might affect the operating system or instrument software. If the instrument software operates incorrectly, consult your facility IT administrator about possible GPO interference.

## Password management

Configure a password that is at least 10 characters, and use local ID policies for additional guidance. Keep a record of the password. For customer security, Illumina does not keep customer login credentials, and unknown passwords cannot be reset. An unknown password requires that an Illumina representative restore the factory default, which removes all data from the system and extends the necessary support time.

## Administrative rights and privileges

Maintain administrative privileges for users. Illumina instrument software is configured to allow user permissions when the instrument is shipped.

**Table 4: Universal approval requirements for internal system operation**

Connection	Value	Purpose
Domain	localhost: <sup>*</sup>	All ports for localhost-to-localhost communication, which are needed for interprocess communication
Port	8081	Real-Time Analysis
Port	8080	Control Software
Port	8090	Remote Copy Service

## Instrument-specific settings

In addition to settings previously mentioned, there are the settings that need to be considered for each platform, representing internal settings that need to be allow-listed.

**Table 5: Information security specifications for Illumina sequencing systems**

System	SRP	EMET	Default IPD setting	Opt-in or Opt-out	IPD setting at software upgrade
NovaSeq	Yes	Yes	On	Opt-out	Retain previous setting
HiSeq	No	No	On	Opt-out	Reset to On
NextSeq	No	No	On	Opt-out	Retain previous setting
NextSeq 550Dx - Research Mode	Yes	Yes	Off	Opt-in	Retain previous setting
NextSeq 1000 and NextSeq 2000	No	No	On	Opt-out	Retain previous setting
MiSeq	No	No	On	Opt-out	Retain previous setting (per user basis)
MiSeqDx	No	No	Off	Opt-in	Retain previous setting
MiSeqDx - Research Mode	No	No	On	Opt-out	Retain previous setting
MiniSeq	No	No	On	Opt-out	Retain previous setting
iSeq 100	Yes	No	On	Opt-out	Retain previous setting
iScan	No	No	On	Opt-out	Retain previous setting (per user basis)

Systems with the LRM module require Port 80 or 443 to be inbound for the local network only

**Table 6: Internal communication requirements by system**

System	Ports and IP addresses	Purpose	Bandwidth requirement
NovaSeq	5555	Hardware controller interface	200 MB/system
NovaSeq	22, 80, 111, 443, 623, 2049, 5900, 8889, 9980, 169.254.x.x, fddc:65e5:66fa::1/48, fddc:65e5:66fa::2/48	Internal data transfer	200 MB/system
HiSeq	The HiSeq System has no internal IP communication processes		100 MB/system
NextSeq	192.168.113.*.*	Allow All Ports. This is the communication link with firmware on the internal network card	50 MB/system
NextSeq 550Dx	192.168.113.*.*	Allow All Ports. This is the communication link with firmware on the internal network card	50 MB/system
NextSeq 550Dx	Port 80 or 443	Local Run Manager. Required local inbound (no internet access)	50 MB/system
NextSeq 1000 and NextSeq 2000	21, 22, 4647, 5458, 5555, 5647, 7359, 7360, 169.254.*.*	Allow All Ports. This is the communication link with firmware on the internal network card	200 MB/system
MiSeq	Port 80 or 443	Local Run Manager. Required local inbound (no internet access)	10 MB/system
MiSeqDx	Port 80 or 443	Local Run Manager. Required local inbound (no internet access)	10 MB/system
MiniSeq	192.168.113.*.*	Allow All Ports. This is the communication link with firmware on the internal network card	10 MB/system
MiniSeq	Port 80 or 443	Local Run Manager. Required local inbound (no internet access)	10 MB/system
iSeq 100	Port 80 or 443	Local Run Manager. Required local inbound (no internet access)	10 MB/system
iScan	6030, 888	AutoLoader	10 MB/system
The IP listed is critical. It is the interface for the hardware controller			

For more information and details on communication requirements, see the Site Prep Guide for the specific system (Table 7). User manuals for each specific system contain information on steps to enable IPD through instrument software (Table 7).

**Table 7: User guides and site prep guides for Illumina systems**

System	User guide	Site prep guide
NovaSeq	<a href="#">1000000019358</a>	<a href="#">1000000019360</a>
HiSeq 1000	<a href="#">15023355</a>	<a href="#">15006407</a>
HiSeq 1500	<a href="#">15035788</a>	<a href="#">15006407</a>
HiSeq 2000	<a href="#">15011190</a>	<a href="#">15006407</a>
HiSeq 2500	<a href="#">15035786</a>	<a href="#">15006407</a>
HiSeq 3000	<a href="#">15066493</a>	<a href="#">15066492</a>
HiSeq 4000	<a href="#">15066496</a>	<a href="#">15066492</a>
HiSeq X	<a href="#">15050091</a>	<a href="#">15050093</a>
NextSeq 500	<a href="#">15046563</a>	<a href="#">15045113</a>
NextSeq 550	<a href="#">15069765</a>	<a href="#">15045113</a>
NextSeq 550Dx	<a href="#">1000000009513</a>	<a href="#">1000000009869</a>
NextSeq 1000/2000	<a href="#">10000000109376</a>	<a href="#">10000000109378</a>
MiSeq	<a href="#">15027617</a>	<a href="#">15027615</a>
MiSeqDx	<a href="#">15070067</a>	<a href="#">15038351</a>
MiniSeq	<a href="#">1000000002695</a>	<a href="#">1000000002696</a>
iSeq 100	<a href="#">1000000036024</a>	<a href="#">1000000035337</a>
iScan	<a href="#">11313539</a>	<a href="#">1000000000661</a>

If a hyperlink becomes inactive due to updates, the provided document number can be used to search the Illumina website for a newer version of the guide

**Instrument performance data types****Table 8: Instrument performance data types (instrument configuration files)**

<b>File name</b>	<b>File description</b>	iScan	HiSeq 1000/1500/2000/2500	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq
Effective.cfg	Software system configuration total parameters	X	X	X	X		X	X	X	X	X	X	X
FirmwareVersions.txt	Firmware version on instrument hardware						X			X	X		X
*Calibration.cfg	Software system calibration parameters	X					X	X		X	X	X	X
*Override.cfg	Software system configuration override parameters	X	X	X	X		X			X	X	X	X
RTAStart.bat	Primary analysis start file					X	X			X	X		
Options.cfg	Software system configuration override parameters												X
*HardwareHistory.csv	Instrument hardware configuration history						X			X	X		
*CurrentHardware.csv	Instrument hardware current configuration						X			X	X		
SequencingConfiguration.xml	Instrument system configuration parameters					X							
Channel*cc.txt	Camera calibration file	X											

**Table 9: Instrument performance data types (instrument operational logs)**

<b>File name</b>	<b>File type</b>	<b>File description</b>	iScan	HiSeq 1000/1500/2000/2500	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq
*.jpg	Run specific operational images	Thumbnail image for each tile and color channel if option has been turned on in software (off by default), usually turned on by FAS/FSE						X	X	X	X	X		
Samplesheet.csv	Run specific sample configuration file													X <sup>a</sup>
Recipe file (XML)	Run specific configuration file	Sequencing recipe used in run				X						X	X	X
Logs.zip		Zipped folder of human readable files; all file readily accessible by customer on instrument					X	X	X	X	X	X	X	X
CompressedLogs.zip		Zipped collection of log files; all files readily accessible by customer on instrument	X											

a. Sample sheet is no longer uploaded in NovaSeq 6000 v1.6 software.

**Table 10: Instrument performance data types (instrument analytics configuration files)**

File name	File description	iScan	HiSeq 1000/1500/2000/2500	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDX	NextSeq	NextSeq 550DX	NextSeq 1000/2000	NovaSeq
RTAConfiguration.xml	RTA configuration	X	X	X	X	X	X	X			X		
RTA3.cfg	RTA configuration				X							X	X
RTAerror.txt	Primary analysis error log file					X	X						

**Table 11: Instrument performance data types (miscellaneous file types)**

File name	File description	iScan	HiSeq 1000/1500/2000/2500	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDX	NextSeq	NextSeq 550DX	NextSeq 1000/2000	NovaSeq
*.IMF logs	Software operational log files		X	X			X				X	X	X
*Results.zip	Service software test results; this is sent only if triggered by a Service & Support personnel in service software					X				X	X	X	

**Table 12: Instrument performance data types (run-specific operational logs)**

File name	File description	iScan	HiSeq 1000/1500/2000/2500	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDX	NextSeq	NextSeq 550DX	NextSeq 1000/2000	NovaSeq
*Firmware_Logs	Firmware operation log files (CSV)					X				X	X		
PreRunDiagnosticFiles	Pre-sequencing run check results and log files (csv and xml)				X	X				X	X	X	X
Cycle Logs	Troubleshooting logs for operational data generated per cycle (txt and xml form)					X	X	X	X	X	X	X	X
*Error*.log	Troubleshooting logs for operational data	X	X	X								X	X
CycleTimes.txt	Cycle duration time during a sequencing run	X	X	X									
UCS Logs	Copy service log file (.json and .csv)												X
CycleTime.tsv	Cycle and scan duration log file	X											
*.scrst	BeadChip scan settings configuration file	X											

**Table 13: Instrument performance data types (run-specific analytics files)**

<b>File name</b>	<b>File description</b>	<b>HiSeq 1000/1500/2000/2500</b>	<b>HiSeq 3000/4000</b>	<b>HiSeq X</b>	<b>iSeq100</b>	<b>MiniSeq</b>	<b>MiSeq</b>	<b>MiSeqDx</b>	<b>NextSeq</b>	<b>NextSeq 550Dx</b>	<b>NextSeq 1000/2000</b>	<b>NovaSeq</b>
RTAComplete.txt	Indicator file that all primary processing has completed	X	X	X	X	X	X	X	X	X	X	X
RTARead*Complete.txt	Indicator file that primary processing has completed key step				X							
RunParameters.xml	Run set up configuration parameters output in XML form at the beginning of the run	X	X	X	X	X	X	X	X	X	X	X
RunInfo.xml	Run set up configuration parameters output in XML form at the beginning of the run used for the Sequencing Analysis Viewer	X	X	X	X	X	X	X	X	X	X	X
RunCompletionStatus.xml	Indicator file indicates sequencing is complete	X	X	X		X	X	X	X	X	X	X
SequenceComplete.txt	Indicator file indicates sequencing is complete											X
*MetricsOut.bin	Binary reporting files for Sequencing Analysis Viewer; not readable by customer without additional software	X	X	X	X	X	X	X	X	X	X	X
AlignmentMetricsOut.bin					X							X
BasecallingMetricsOut.bin					X							X
CorrectedIntMetricsOut.bin	Average intensity, corrected channel intensity, corrected called intensity, called counts	X	X	X	X	X	X	X	X	X	X	X
EmpiricalPhasingMetricsOut.bin	Phasing, Prephasing per cycle	X	X	X	X	X	X	X	X	X	X	X
ErrorMetricsOut.bin	Error rate, read errors	X	X	X	X	X	X	X	X			X
EventMetricsOut.bin	Timing data for RTA started, cycle started, template generation started/completed, posttemplate max clusters init, system memory available gigabyte, registration and extraction, neighbor correction, color matrix correction, template generation, base calling and quality scoring, sequence alignment, bclwriting, read started/completed, filter align started/completed, cycle completed, RTA completed	X	X	X	X	X	X	X	X	X	X	X
ExtendedTileMetricsOut.bin					X							X
ExtractionMetricsOut.bin	Focus scores, intensities, time	X	X	X	X		X	X	X	X	X	X
FWHMGridMetricsOut.bin					X							X
ImageMetricsOut.bin					X							X
IndexMetricsOut.bin	Name, sample name, project name				X		X					X
OpticalModeMetricsOut.bin												X
PFGrtidMetricsOut.bin	Cluster count, PF cluster count, Locs area in mm^2	X	X	X	X		X	X	X	X	X	X
QMetrics2030Out.bin					X		X					X
QMetricsByLaneOut.bin					X		X					X
QMetricsOut.bin	Q-score histogram	X	X	X	X		X	X	X			X
RegistrationMetricsOut.bin	Subtile offsets, affine transform	X	X	X			X	X	X			X
TileMetricsOut.bin	Cluster density, cluster density PF, cluster count, cluster count PF, percent aligned, percent phasing, percent prephasing, latest extracted cycle, latest called cycle, latest Q-scored cycle, latest error cycle	X	X	X	X		X	X	X	X	X	X
*.tsv or *.txt	TSV or TXT log files generated for RTA file copy logs, global logs, and warning logs; accessible by the customer in human readable form				X		X	X	X	X		
QGridMetricsOut.bin					X							
ReconstructionMetricsOut.bin												X

## References

1. Microsoft Security TechCenter. [portal.msrc.microsoft.com/en-us/](http://portal.msrc.microsoft.com/en-us/). Accessed December 19, 2017.
2. Announcing the Advanced Encryption Standard (AES). [www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-secure-mobility-client/fips.pdf](http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-secure-mobility-client/fips.pdf). Accessed December 19, 2017.
3. AWS: ISO 27001. [aws.amazon.com/compliance/iso-27001-faqs/](http://aws.amazon.com/compliance/iso-27001-faqs/). Accessed June 4, 2018.
4. IBM: Transform your business with the GDPR. [www.ibm.com/data-responsibility/gdpr/#commitment-to-readiness?cm\\_mmc=Search\\_Google\\_-\\_Security\\_CISO\\_-\\_WW\\_NA\\_-\\_gdpr\\_Exact\\_-&cm\\_mmca2=10006807&cm\\_mmca7=9061191&cm\\_mmca8=kwd-296891238925&cm\\_mmca9=\\_kenshoo\\_clickid\\_&cm\\_mmca10=272585904650&cm\\_mmca11=e&mkwid=\\_kenshoo\\_clickid\\_&cvo\\_src=ppc.google.&cvo\\_campaign=000026XZ&cvo\\_crid=272585904650&Matchtype=e](http://www.ibm.com/data-responsibility/gdpr/#commitment-to-readiness?cm_mmc=Search_Google_-_Security_CISO_-_WW_NA_-_gdpr_Exact_-&cm_mmca2=10006807&cm_mmca7=9061191&cm_mmca8=kwd-296891238925&cm_mmca9=_kenshoo_clickid_&cm_mmca10=272585904650&cm_mmca11=e&mkwid=_kenshoo_clickid_&cvo_src=ppc.google.&cvo_campaign=000026XZ&cvo_crid=272585904650&Matchtype=e). Accessed June 4, 2018.
5. Illumina (2016) BaseSpace Sequence Hub Security and Privacy. ([www.illumina.com/content/dam/illumina-marketing/documents/products/whitepapers/basespace-sequence-hub-security-and-privacy-white-paper-970-2016-020.pdf](http://www.illumina.com/content/dam/illumina-marketing/documents/products/whitepapers/basespace-sequence-hub-security-and-privacy-white-paper-970-2016-020.pdf)).
6. Illumina (2016) BaseSpace Variant Interpreter and HIPAA. ([www.illumina.com/content/dam/illumina-marketing/documents/products/technotes/basespace-variant-interpreter-HIPAA-technical-note-970-2016-003.pdf](http://www.illumina.com/content/dam/illumina-marketing/documents/products/technotes/basespace-variant-interpreter-HIPAA-technical-note-970-2016-003.pdf)).
7. Illumina (2016) Illumina Security Best Practices Guide. ([www.illumina.com/content/dam/illumina-marketing/documents/products/guides/illumina-security-best-practices-guide-970-2016-016.pdf](http://www.illumina.com/content/dam/illumina-marketing/documents/products/guides/illumina-security-best-practices-guide-970-2016-016.pdf)).